5th Annual IT Security Automation Conference and Expo

October 26 - 29, 2009, Baltimore Convention Center

Focusing on Healthcare IT, Cyber Security, Regulatory Compliance, and other Emerging Secure IT Technologies

Conference Agenda

Day 1, Monday, October 26

	SCAP Introduction	**BENCHMARK DEVELOPMENT COURSE (T)**	**NIST/ISALLIANCE VOIP SCAP PROJECT - PHASE II KICKOFF**
	Room 316/317	Room 318/319	Room 320
8:30 - 9:00 am	*Registration*		
9:00 - 9:15 am	**Welcome**	**Welcome**	
9:15 - 9:45 am	**SCAP Introduction (T)**	**Phase 1: Writing Good Guidance**	
9:45 - 11:00 am		**Phase 2: Augmenting Recommendations using SCAP**	
11:00 - 11:15 am	*Break*		
11:15 am - 12:15 pm	**SCAP Introduction (T)**	**Phase 3: Checking Language Overview (T)**	
12:15 - 1:30 pm	*Lunch*		
1:30 - 2:45 pm	**Making Security Measurable (T)**	**Phase 4: Introduction to Creating Checks (T)**	**ISAlliance Phase II Kickoff Workshop**
2:45 - 3:00 pm	*Break*		
3:00 - 4:00 pm	**OCIL Introduction (T)**	**Phase 5: Benchmark Structure and Tailoring with XCCDF (T)**	**ISAlliance Phase II Kickoff Workshop (continued)**
4:00 - 4:30 pm		**Phase 6: Using Benchmarks and Wrap-up (T)**	

Day 2, Tuesday, October 27

	Plenary Sessions				
	Ballroom I				
7:30 - 9:00 am	*Registration, Foyer*				
9:00 - 9:10 am	**Conference Welcome Address – Cita Furlani, NIST**				
9:10 - 9:55 am	**Keynote – Phil Reitinger, Deputy Undersecretary, DHS**				
9:55 - 10:15 am	**NIST Address – Tim Grance, NIST**				
10:15 - 10:35 am	*Break, Vendor Expo Hall*				
10:35 - 11:10 am	**Symantec Address – John Thompson, Chairman of the Board and former CEO, and Mark Bregman, CTO, Symantec**				
11:10 - 11:45 am	**RSA Address – Mischel Kwon, Vice President Public Sector Security Solutions of RSA, The Security Division of EMC**				
11:45 am - 12:15 pm	**Overview of Tracks – Track leads**				
12:15 - 1:15 pm	*Lunch, Vendor Expo Hall*				
	SCAP	**DOD SECURITY AUTOMATION STRATEGY AND ACTIVITIES**	**HEALTH IT AND FIPS**	**COMPUTER NETWORK MONITORING, AUDIT, AND LOGGING**	**CLOUD COMPUTING**
	Ballroom I	Room 316/317	Room 318/319	Room 324/325	Ballroom II
1:15 - 1:45 pm	**Security Automation Through Granular Change Detection** – Jim Ivers, Triumfant	**DoD Opening Discussion**	**NIST HIT Test Infrastructure Project** – Rob Snelick, NIST	**Insider Threat Panel** – Bruce Gabrielson, Moderator	**A Vision for a Private Cloud** – David Hunter, VMWare, Kunjal Trivedi, Cisco, and Nicklous Combs, EMC Federal
1:45 - 2:15 pm	**Automating Vulnerability Management at Orbitz with SCAP** – Ed Bellis, Orbitz	**Consensus Audit Guidelines (CAG)** – Mason Brown, SANS	**Architecting Measurable Security in Health Information Technology Using SCAP** – Kenneth Lin, Booz Allen Hamilton	**Developing an SCAP Solution for Unified Communications** – Lawrence Dobranski, Nortel Networks, John Nagengast, AT&T, and Ben Halpert, Lockheed Martin	**A Vision for a Private Cloud (continued)** – David Hunter, VMWare, Kunjal Trivedi, Cisco, and Nicklous Combs, EMC Federal
2:15 - 2:45 pm	**BigFix's Experience with Standards** – Jim Hansen, BigFix	**ARF, ARCAT, and Summary Reporting (T)** – LtCol Wolfkiel, NSA	**Centers for Medicare and Medicaid Services Case Study** – Ryan Brewer, CMS CISO	**Using SCAP for Automated VoIP Configuration, Assurance and Security** – Paul Sand, Salare Security, LLC	**App-Centric Scalability, Reliability, and Security in the Cloud** – Prakash Sinha, Citrix

Day 2, Tuesday, October 27					
2:45 - 3:15 pm	**Industry Standards: The Key to Deploying a Closed-Loop Process for Endpoint Policy Compliance** – Rajat Bhargava, StillSecure and Tom Lerach, HP	**ARF, ARCAT, and Summary Reporting (T) (continued)** – LtCol Wolfkiel, NSA	**Centers for Medicare and Medicaid Services Case Study (continued)** – Ryan Brewer, CMS CISO	**Baseline Standards for Applying SCAP to Secure VoIP** – Mark Humphrey, Boeing, and Scott Armstrong, Gideon Technologies	**Security Challenges in Cloud Computing** – Hasan S. Alkhatib, Microsoft
3:15 - 3:30 pm	*Break, Vendor Expo Hall*				
3:30 - 4:00 pm	**Situational Awareness *Secure Ops** – Tiffany Jones, Symantec	**CND Data Strategy (T)** – Shawn Oles and Sandra Harrell-Cook, NSA	**Cryptographic Transition Strategies** – Tim Polk, NIST	**Common Event Expression (CEE) (T)** – Bill Heinbockel, Mitre	**An Accredited Fed Cloud IaaS** – Pete Nicoletti, Terremark
4:00 - 4:30 pm	**Next Generation SCAP: Threat Intelligence Scoring and XML Reporting Standards** – Jonathan Couch, iSight	**CND Data Strategy (T) (continued)** – Shawn Oles and Sandra Harrell-Cook, NSA	**Cryptographic Validation Programs** – Randy Easter and Sharon Keller, NIST	**Log Standard Challenges** – Anton Chuvakin	**Cloud Standards: Opening the Cloud** – Victor L. Harrison, Object Management Group (OMG) Board of Directors
4:30 - 5:00 pm	**Securing the Enterprise Panel** – Kim Watson, Moderator	**Expanding the Use of SCAP: Malware Detection and MACE Tool Demo (T)** – Paul Green and George Saylor, G2	**Cryptographic Validation Programs (continued)** – Randy Easter and Sharon Keller, NIST	**NSA Audit Management** – Chip Lutz, Booz Allen Hamilton	**Separating Perceptional from Real Security Concerns** – George Reese, enStratus
5:00 - 5:30 pm	**Securing the Enterprise Panel (continued)** – Kim Watson, Moderator	**Expanding the Use of SCAP: Malware Detection and MACE Tool Demo (continued) (T)** – Paul Green and George Saylor, G2	**Secure and Scalable RESTful Health Data Exchange** – Gerald Beuchelt, MITRE	**Final Thoughts** – Kevin Bingham, NSA	**Why Automation and Interoperability is Critical to Cloud Success** – Charles Crouchman, Opalis
5:30 - 7:00 pm	**Reception, Vendor Expo Hall and Foyer**				

Day 3, Wednesday, October 28

	Plenary Sessions				
	Ballroom I				
8:00 - 8:50 am	*Registration, Foyer*				
8:50 - 9:00 am	**Opening Remarks**				
9:00 - 9:45 am	**Keynote – Tony Sager, NSA**				
9:45 - 10:30 am	**DoD Address – Richard Hale, DISA**				
10:30 - 10:50 am	*Break, Vendor Expo Hall*				
10:50 - 11:20 am	**Next Generation Risk Management – Ron Ross, NIST**				
11:20 am - 12:20 pm	**Operating System Vendor Panel – Mischel Kwon, Moderator**				
12:20 - 1:30 pm	*Lunch, Vendor Expo Hall*				
	SCAP	**DOD SECURITY AUTOMATION STRATEGY AND ACTIVITIES**	**COMPLIANCE FRAMEWORKS/ 800-53/FISMA**	**SCAP TECHNICAL**	**CLOUD COMPUTING**
	Ballroom I	Room 316/317	Room 318/319	Room 324/325	Ballroom II
1:30 - 2:00 pm	**Microsoft Adoption of SCAP** – Kelly Hengesteg and Chase Carpenter, Microsoft	**HBSS Open Framework Strategy** – Mark Orndorff	**Understanding the Greatest FDCC Technical Challenges (T)** – Kurt Dillard	**Content Validation (T)** – Andy Bove, Secure Acuity	**Into the Cloud with SCAP** – Ron Knode, CSC
2:00 - 2:30 pm	**The OpenSCAP Project** – Steve Grubb, RedHat and Kevin Sitto, G2	**VMS/STIG SCAP Strategy (T)** – David Hoon, DISA	**Understanding the Greatest FDCC Technical Challenges (T) (continued)** – Kurt Dillard	**Semantic Technologies Primer (T)** – Tim Keanini, nCircle	**Using SCAP to Mitigate Risks in the Cloud** – Ron Ritchey, Booz Allen Hamilton
2:30 - 3:00 pm	**Public Sector Adoption of SCAP Panel** – Paul Bartock, Moderator	**VMS/STIG SCAP Strategy (T) (continued)** – David Hoon, DISA	**FISMA Implementation Project Update** – Arnold Johnson	**Semantic Technologies Primer (T) (continued)** – Tim Keanini, nCircle	**Security as a Service** – Scott Chasin, McAfee
3:00 - 3:15 pm	*Break, Vendor Expo Hall*				
3:15 - 3:45 pm	**Automating the Continuous Compliance Process in the Decentralized Enterprise** – Bill Niester, Qualys	**Automating Attack Analysis Using Audit Data (T)** – Bruce Gabrielson, Booz Allen Hamilton	**FDCC Compliance and Audit** – Kent Landfield, McAfee	**Semantic Engineering and Modeling Panel (T)** – Dave Waltermire, Moderator	**New Advances in Virtualization Security Enable Secure Cloud Computing** – Aaron Bawcom, Reflex Systems

Day 3, Wednesday, October 28

3:45 - 4:15 pm	**Automating Network Security Assessment** – Dr. Mike Lloyd, RedSeal Systems, Inc. and Doug Dexter, Cisco	**NETSPA (T)**	**FDCC Compliance and Audit (continued)** – Kent Landfield, McAfee	**Semantic Engineering and Modeling Panel (T) (continued)** – Dave Waltermire, Moderator	**Cloud-enabled Protection of Data Integrity and Authenticity of Electronic Content** – Tom Klaff, Surety, LLC
4:15 - 4:45 pm	**Enhancing SCAP with Whitelist-based Image Management** – Wyatt Starns, SignaCert	**NSA Digital Policy** – Peter Sell	**SCAP – Lessons Learned and an Enterprise Use Case** – Tony Uceda-Velez, Gideon Technologies	**Semantic Engineering and Modeling Panel (T) (continued)** – Dave Waltermire, Moderator	**Endpoint Data Protection Services** – Gary Sumner, DataCastle Corporation
4:45 - 5:15 pm	**Vendor Interoperability Panel** – Andy Bove, Moderator	**Remediation Specification (T)** – Matt Wojcik, Mitre	**National Information Assurance Engagement Center (NIAEC)** – Wende Peters, Johns Hopkins APL	**Relational Database to Triple Store Migration (T)** – Vaibhav Khadilkar and Jyothsna Rachapalli, University of Texas at Dallas	**The Cloud Architecture Transformation** – Jim Blakley, Intel Corporation

Day 4, Thursday, October 29

	SCAP Workshops	**Security Automation Workshops**
	Room 316/317	Room 318/319
8:30 - 9:00 am	*Registration*	
9:00 - 9:15 am	**Welcome**	**Welcome**
9:15 - 10:45 am	**The Future of CPE (T)**	**Software Assurance Automation (T)**
10:45 - 11:00 am	*Break*	
11:00 am - 12:00 pm	**XCCDF Technical Deep-Dive for Next Version (T)**	**ISO, ITU, Common Criteria, and the Content Automation Efforts (T)**
12:00 - 1:15 pm	*Lunch*	
1:15 - 3:15 pm	**XCCDF Technical Deep-Dive for Next Version (T)**	**OpenSCAP (T)**
3:15 - 3:30 pm	*Break*	
3:30 - 4:30 pm	**Where we Stand with Remediation (T)**	**Malware Attribute Enumeration and Characterization (MAEC) Introduction (T)**

5th Annual IT Security Automation Conference and Expo

October 26 - 29, 2009, Baltimore Convention Center

Focusing on Healthcare IT, Cyber Security, Regulatory Compliance, and other Emerging Secure IT Technologies

Plenary Session Speakers

Cita Furlani, Director, Information Technology Laboratory
National Institute of Standards and Technology

Cita M. Furlani is Director of the Information Technology Laboratory (ITL). ITL is one of nine research Laboratories within the National Institute of Standards and Technology (NIST) with an annual budget of $85 million, 335 employees, and about 150 guest researchers from industry, universities, and foreign laboratories. Furlani has several leadership responsibilities in addition to those at NIST. Currently, she is Co-Chair of the Interagency Working Group on Digital Data, Co-Chair of the Subcommittee on Quantum Information Science, and Co-Chair for Strategic Planning for the Subcommittee on Networking and Information Technology Research and Development, all under the auspices of the National Science and Technology Council. She also serves as Co-Chair of the Technology Infrastructure Subcommittee of the Interagency CIO Council.

Furlani has served as the Chief Information Officer (CIO) for NIST. As CIO, Furlani was the principal adviser to the NIST Director on the planning, execution, evaluation, and delivery of information technology services and support. She earned a Master of Science degree in electronics and computer engineering from George Mason University and a Bachelor of Arts degree in physics and mathematics from Texas Christian University. She was awarded two Department of Commerce Bronze Medal Awards in 1985 and 1993 and the Department of Commerce Silver Medal Award, in 1995.

Phil Reitinger, Deputy Undersecretary
Department of Homeland Security

Philip Reitinger is the Deputy Undersecretary of the Department's National Protection and Programs Directorate (NPPD). In this role he is charged with protecting the U.S. government's computing systems from domestic and foreign threats. Mr. Reitinger previously served as Chief Trustworthy Infrastructure Strategist at Microsoft Corp., where he was responsible for helping improve the protection and security of the critical information technology infrastructure. That role allowed him to coordinate closely with government agencies and private partners on cybersecurity protection programs to build trustworthy computing systems worldwide.

As a current member of the Federal Emergency Management Agency (FEMA) National Advisory Council, Reitinger advises the FEMA administrator on aspects of cyber security related to emergency management. He is an expert on computer crime and policy, and previously was the Executive Director of the U.S. Department of Defense's (DOD) Cyber Crime Center, charged with providing electronic forensic services and supporting cyber investigative functions department-wide. Before joining DOD, Reitinger served as Deputy Chief of the Computer Crime and Intellectual Property division at the U.S. Department of Justice.

Reitinger holds a law degree from Yale Law School and a bachelor's degree in electrical engineering and computer science from Vanderbilt University.

Tim Grance, Senior Computer Scientist, Information Technology Laboratory National Institute of Standards and Technology

Tim Grance is a senior computer scientist in the Information Technology Laboratory at the National Institute of Standards and Technology. He leads team of researchers in the Systems and Network Security Group and is engaged in a broad research program focused on such topics as cloud computing, access control, identity management, vulnerability analysis, privacy protections, security metrics, protocol security, smart cards, and wireless/mobile device security. In addition, he is also the Program Manager for Cyber and Network Security (CNS) Program and exercises broad technical and programmatic oversight over the NIST CNS portfolio. This portfolio includes high profile projects such as the NIST Hash Competition, Cloud Computing, Security Content Automation Protocol (SCAP), Protocol Security (DNS, BGP, IPv6), Combinatorial Testing, and the National Vulnerability Database.

He has extensive public and private experience in accounting, law enforcement, and computer security. He has written on diverse topics including incident handling, intrusion detection, privacy, metrics, contingency planning, forensics, and identity management. He was named in 2003 to the Fed 100 by Federal Computer Week as one of the most influential people in Information Technology for the US Government. He is also is a recipient of the highest award from the US Department of Commerce — a Gold Medal, from the Secretary of Commerce.

John Thompson, Chairman of the Board Symantec Corporation

John W. Thompson is chairman of the board of directors of Symantec Corporation. During his 10-year tenure as chief executive officer, he helped transform Symantec into a leader in security, storage and systems management solutions delivered to a broad base of customers, from individual consumers to the largest enterprises in the world.

With a broad range of business, civic and philanthropic interests, Thompson has been involved in a number of important projects primarily focused on infrastructure protection and the development of our nation's youth. In September 2002, President George W. Bush appointed Thompson to the National Infrastructure Advisory Committee (NIAC), to make recommendations regarding the security of the critical infrastructure of the United States. In addition, Thompson has served as the chair of the Silicon Valley Blue Ribbon Task Force on Aviation Security and Technology to identify and evaluate technology-driven solutions to improve the security and efficiency of national and local aviation. He serves on the national board of Teach for America, an organization dedicated to eliminating educational inequities for all children and in 2008 was inducted into the Junior Achievement Business Hall of Fame.

On the business front, Thompson serves on the board of JovianDATA, an early stage company focused on delivering advanced business analytic services to a rapidly growing on-line advertising market. He also serves as a director on the boards of UPS, the world leader in global logistics, and Seagate Technology, the world leader disk-drive development and manufacturing.

Thompson completed his undergraduate studies at Florida A&M University and holds a master's degree in management science from MIT's Sloan School of Management. In addition, in May 2008, he received an honorary doctorate degree from Notre Dame University.

Mark Bregman, Executive Vice President and CTO Symantec Corporation

Mark Bregman is executive vice president and chief technology officer at Symantec, responsible for the Symantec Research Labs, Symantec Security Response and shared technologies, emerging technologies, architecture and standards, localization and secure coding, and developing the technology strategy for the company. Bregman guides Symantec's investments in advanced research and is responsible for the company's development centers in India and China.

Additionally, Bregman leads the field technical enablement team, which works closely with the technical sales team to ensure they are prepared to assist customers in managing the impact of changing and emerging technical requirements.

Bregman joined Symantec through the company's merger with Veritas Software, where he served as chief technology officer, responsible for cross-product integration, advanced product development, merger and acquisition strategy, and the company's engineering development centers in India and China.

Prior to joining Veritas, Bregman was CEO of Airmedia, a wireless Internet firm. Previously, Bregman spent 16 years at IBM where he led the RS/6000 and Pervasive Computing divisions and held senior management positions in IBM Research and IBM Japan. He was also technical assistant to IBM CEO Lou Gerstner.

Bregman holds a bachelor's degree in physics from Harvard College and a master's degree and doctorate in physics from Columbia University. He is a member of the Visiting Committee to the Harvard University Libraries, a member of the American Physical Society, and a senior member of IEEE. He also serves on the Board of Directors of ShoreTel and the Bay Area Science and Innovation Consortium.

Mischel Kwon, Vice President Public Sector Security Solutions of RSA, The Security Division of EMC

Mischel Kwon is Vice President of Public Sector Security Solutions for the Worldwide Professional Services unit at RSA, The Security Division of EMC. In this role, Ms. Kwon is responsible for leading RSA's Security Consulting Services practice. While focusing on the public sector, she also provides private sector customers and global organizations strategic, technical and policy assistance in building, defending, identifying, and remediating their critical infrastructures against cyber threats, attacks and vulnerabilities.

Ms. Kwon has more than 27 years of information technology experience, with expertise and leadership in the design, implementation and management of critical IT infrastructure and security operations programs. Prior to joining RSA, Ms. Kwon was the Director for the United States Computer Emergency Readiness Team (US-CERT), where she spearheaded the organization responsible for analyzing and reducing cyber threats and vulnerabilities in federal networks, disseminating cyber threat warning information and coordinating national incident response activities. In addition, she previously served as the Deputy Director for IT Security Staff at the United States Department of Justice (DOJ) where she built and deployed the Justice Security Operations Center (JSOC) to monitor and defend the DOJ network against cyber threats.

Tony Sager, Chief of the Vulnerability Analysis and Operations Group. National Security Agency

Tony Sager is the Chief of the Vulnerability Analysis and Operations (VAO) Group within the Information Assurance Directorate at the National Security Agency. VAO's mission is to identify and analyze the vulnerability of information, technology, and operations for NSA customers, primarily within the Defense Department and the Intelligence Community. VAO is also very active in helping the broader national security community deal with these same problems through guidance and standards. During the last year, VAO has received recognition from several private sector sources (including SC Magazine Editor's Choice for 2007; and The National Information Security Leadership Award from Government Executive Magazine and the SANS Institute).

During his 30 year career at the NSA, Tony has held a number of technical and managerial positions in Computer/Network Security and software analysis. He holds a BA in Mathematics from Western Maryland College and an MS in Computer Science from the Johns Hopkins University. Tony is also a graduate of the US Army Signal Officer Basic Course (as a civilian), and the National Security Leadership Course. He is in constant demand to be the keynote speaker at national and international security events.

Richard Hale, Chief, Communications Information Assurance Engineering & Support Defense Information Systems Agency

Richard Hale oversees Information Assurance (IA) engineering and support for the Defense Information Systems Agency. In this position he is responsible for coordinating the design and implementation of a defense-in-depth strategy across the DISA managed information infrastructure and across DISA developed systems.

He previously worked at the Naval Research Laboratory where he participated in the design and analysis of a variety of Navy and Department of Defense information and communication systems.

He holds Bachelor's degrees in Applied Mathematics and Electrical Engineering and a Master's degree in Electrical Engineering, both from the University of Virginia.

Ron Ross, Senior Computer Scientist and Information Security Researcher National Institute of Standards and Technology

Dr. Ron Ross is a senior computer scientist and information security researcher at the National Institute of Standards and Technology (NIST). His current areas of specialization include security requirements definition, testing and evaluation, risk management, and information assurance. Ross leads the Federal Information Security Management Act Implementation Project for NIST, which includes the development of key security standards and guidelines for the federal government, support contractors, and the United States critical information infrastructure. Ross is also the principal architect of the NIST Risk Management Framework that provides a disciplined and structured methodology for integrating the suite of FISMA security standards and guidelines into a comprehensive enterprise-wide information security program.

Paul Bartock
National Security Agency

Paul Bartock is the Technical Director for Information Assurance Transformation for the Vulnerability Analysis and Operations Group, as well as the Program Director for the Defense Industrial Base in the Information Assurance Directorate at NSA. He is responsible for working with DoD, federal government and private industry stakeholders to promote the use of security standards and best practices. He provided technical guidance on the government work groups to influence the development of the security baseline configurations, which led to the OMB-mandated Federal Desktop Core Configuration. Drawing on his extensive knowledge of networks, he developed countermeasure guidance to mitigate vulnerabilities in DOD and DIB networks. Mr. Bartock is a graduate of University of Maryland and is a Certified Information Systems Security Professional and a Network Certified Engineer. In November 2008, he received the Exceptional Civilian Service Award for his work developing stakeholder consensus on the federal security baselines.

John Banghart, SCAP Validation Program Manager
National Institute of Standards and Technology

John Banghart has spent over 15 years in the IT/IS fields, both in the private and public sectors. Currently, he is the SCAP Validation Program Manager at the National Institute of Standards and Technology (NIST). As part of the broader security automation initiative, this program develops software requirements and accredits laboratories for the purpose of validating that products are correctly implementing the Security Content Automation Protocol (SCAP). John is currently the NIST representative to the Interagency Security Automation Program (ISAP) working group, where he works with other agency representatives and external stakeholders to develop and promote security automation initiatives across the federal government and private sector.

5th Annual IT Security Automation Conference and Expo

October 26 - 29, 2009, Baltimore Convention Center

Focusing on Healthcare IT, Cyber Security, Regulatory Compliance, and other Emerging Secure IT Technologies

SCAP Track Abstracts

Day 2, Tuesday, October 27	
	Over the past several years, security automation has evolved through collaboration and application among DoD, federal agencies, and private industry partners. Instead of developing proprietary solutions to measure and manage vulnerability and compliance information, an increasing number of commercial companies today are using SCAP standards and protocols to automate security. This track will present various presentations on how vendors are taking the lead to develop innovative SCAP–based solutions. This includes assessing vulnerability risk, base-lining the health of the system, improving operational security and identifying the threat risk. Vendors will discuss their specific solutions and will present case studies on how they are improving security for customers.
	Ballroom I
1:15 - 1:45 pm	**Security Automation Through Granular Change Detection** – Jim Ivers, Triumfant For some time, security tools have ground to a halt mid-way through the detect to act cycle requiring intervention by skilled security personnel to complete the analysis and build the scripts to remediate the detected problems. That is because traditional tools only look at problems in the context of the endpoint and require some knowledge of the attack. Capturing every elemental change to the machine and analyzing those changes in the broader context of the endpoint population provides the missing dimension needed to fully automate the detect to act cycle – including the ability to synthesize situational remediations on the fly without the need for human intervention. This presentation will show how collecting, analyzing and correlating granular changes can be put to practical application to detect and remediate malicious attacks and automate continuous enforcement of configurations and policies. Jim Ivers, Chief Marketing Officer, is responsible for worldwide marketing and product management at Triumfant. Ivers and has over 25 years of experience in the IT industry with a background that spans security, integration, business intelligence and application development.
1:45 - 2:15 pm	**Automating Vulnerability Management at Orbitz with SCAP** – Ed Bellis, Orbitz Orbitz Worldwide is made up of many online travel brands and platforms around the globe. The size and complexity of these web applications and the infrastructure that support them have required a best of breed approach in vulnerability assessment tools and services. This approach has enabled Orbitz to choose tools that best fit the job and platform they are dedicated to, but creates chaos in managing an unruly amount of data in silos using different processes, language and processes. Enter SCAP. Orbitz Worldwide partnered with HoneyApps, to create a centralized vulnerability management system built on SCAP standards to correlate and prioritize our data and automate the vulnerability management workflow throughout the organization without replacing our existing tool-sets. Ed is the Chief Information Security Officer responsible for the protection and security of all information and electronic assets as well as compliance and ethics across the wide array of business units that make up Orbitz Worldwide on a global basis. These assets include Orbitz, CheapTickets, eBookers, Away.com, HotelClub, RatesToGo, AsiaHotels, and Orbitz for Business.

Day 2, Tuesday, October 27	
2:15 - 2:45 pm	**BigFix's Experience with Standards** – Jim Hansen, BigFix When it comes to specific IT guidelines for regulatory compliance, mandates like FISMA, HIPAA, NERC, and even PCI DSS are notoriously vague and open to interpretation. This results in uncertainty, inconsistency, and downright panic for IT security teams when it's time to be measured during audit. Clearly, more direction is needed. Unlike other regulatory standards, the FDCC (Federal Desktop Core Configuration), maintained by NIST and mandated by the OMB for all federal agencies, provides highly detailed direction on the security configuration of all desktops within the networks of federal agencies. IT security staff from federal and commercial organizations attending this session will be provided a detailed overview of FDCC and SCAP from the perspective of a vendor, information on how some federal agencies are managing their FDCC projects, information on how organizations can benefit from adopting the standard and best practices for implementing and assessing against FDCC - at low cost, with rapid roll-out. Jim Hansen is a Product Management Director for BigFix, focused on developing market-leading, differentiated security and compliance solutions for large and medium sized enterprise organizations and federal agencies.
2:45 - 3:15 pm	**Industry Standards: The Key to Deploying a Closed-Loop Process for Endpoint Policy Compliance** – Rajat Bhargava, StillSecure and Tom Lerach, HP Regulatory policies, cybersecurity threats, financial loss, and operational control are motivating agencies to institute endpoint policy compliance. Unfortunately, existing approaches that utilize standalone tools are unable to provide accurate, unbiased, real-time information about an agency's endpoint security posture. This presentation will discuss how a next generation, closed-loop methodology is needed to effectively deploy endpoint policy compliance. The presentation will cover the closed-loop process for endpoint policy compliance and common languages needed allow various technologies to talk to each other. Technologies covered will include network access control, LDAP, RADIUS servers, switches, patch managers, and others. The presentation will also cover standards for endpoint policy compliance, including FDCC, OVAL, CVE, and SCAP. When deployed correctly, this closed-loop process occurs with each endpoint's network connect, 24x7x365. The results are a secure network, reduced costs, and clear visibility of the agency's security posture. As Chief Executive Officer, Rajat Bhargava brings a wealth of entrepreneurial experience to his role with StillSecure. Mr. Bhargava is responsible for defining the company's vision and strategy as well as executing on that vision. Tom Lerach is a senior executive with more than 15 years experience in the Information Technology field at EDS, an HP company. His current role is Executive Director for NMCI Operations overseeing the business health and delivery of enterprise programs for the NMCI Contract and the delivery of Information Assurance services providing secure and universal information technology access to more than 700,000 users in the Navy and Marine Corps at over 300 locations across the United States as well as sites in the Far East and Puerto Rico.
3:15 - 3:30 pm	*Break, Vendor Expo Hall*
3:30 - 4:00 pm	**Situational Awareness *Secure Ops** – Tiffany Jones, Symantec This presentation will discuss the basic SCAP objectives for assisting with the cyber situational awareness problem, adoption trends of SCAP, identifying some gaps that still exist to make broader adoption a reality, and various use cases as we think about other ways SCAP can be applied to obtain better situational awareness. Tiffany Jones is the Director of Cyber Strategy, Policy and Programs for Symantec Corporation. Ms. Jones is currently an officer on the IT-Sector Coordinating Council, ex-officio Chair of the TechAmerica Information Security Committee, and serves on several public-private advisory panels. Prior to working for Symantec, Ms. Jones served as Deputy Chief of Staff for the President's Critical Infrastructure Protection Board at the White House.

Day 2, Tuesday, October 27	
4:00 - 4:30 pm	**Next Generation SCAP: Threat Intelligence Scoring and XML Reporting Standards** – Jonathan Couch, iSight SCAP standards today handle a wide variety of technical reporting and communications between systems that deal primarily with vulnerability intelligence and systems configuration. However, what about threat intelligence that incorporates not only technical information but threat actor, tradecraft, skill levels and other non-technical pointers that build on the technology being used? This talk explores the beginning of two areas that build upon CVSS and SCAP: threat scoring and XML standards for threat intelligence reporting. For threat scoring we propose and outline a prototype CVSS-like system for measuring the risk posed by a technology and/or threat actor. XML standards will explore what specific tags will be required for future report delivery. XML tags should support full report delivery (e.g., articles), yet provide a construct for the reporting to be broken up, transmitted, stored and organized in order to leverage individual data elements and metadata within the reports. This information is not only useful for searching of data, but will eventually allow for integration into current SCAP-capable systems to add context to the technical information and the eventual development of threat signatures based on observed tradecraft of technical attacks. Jonathan Couch is currently the Chief Technology Officer for iSIGHT Partners, a global risk management & mitigation firm formed in 2006. Jonathan oversees innovative technology development and strategic technology partnerships for iSIGHT Partners, applying his unique experience in converged security to commercial interests abroad.
4:30 - 5:00 pm	**Securing the Enterprise Panel** – Kim Watson, Moderator The U.S. federal government networks are among those most targeted by professional attacks, including criminal parties and even foreign governments. For this reason Belarc and others are proposing a new framework of continuous monitoring of automated security controls, such as those in the recent Consensus Audit Guidelines. In addition, Belarc is suggesting that the monitoring and remediation functions should be separated. Remediation should be done on a local basis, whereas monitoring should be on an enterprise wide basis. This will allow each task to be done in the best way possible. Remediation can be done by the local admins at the right time and place. Monitoring can then be done in a fully automated way, enterprise-wide, and based on standards. Panelists include Sumin Tchen, Co-Founder of Belarc, John Pescatore, VP Internet Security, Gartner, Inc., and Wyatt Starnes, Founder and CEO of SignaCert, Inc.
5:00 - 5:30 pm	**Securing the Enterprise Panel (continued)** – Kim Watson, Moderator

Day 3, Wednesday, October 28	
	Ballroom I
1:30 - 2:00 pm	**Microsoft Adoption of SCAP** – Kelly Hengesteg and Chase Carpenter, Microsoft This presentation will address Microsoft's efforts to support the SCAP data formats including progress to date and future plans. Kelly's team published the System Center Configuration Manager Extensions for SCAP in July, she will give details on how the Extensions are being used by federal agencies to document FDCC compliance using NIST's SCAP content. She will also provide a preview of the Security Compliance Manager (SCM), a tool Microsoft has been using to centrally organize technical information about every setting that appears in Microsoft's security guidance for Windows and Office. When SCM is released early next year anyone will be able to use it for reviewing Microsoft security baselines and exporting them as configuration packs for System Center Configuration Manager, SCAP content, Excel workbooks, and group policy objects ready for import into Active Directory. Organizations will also be able to customize the settings of the baselines included in SCM to fit their unique requirements. Kelly Hengesteg is a Principal Group Manager on the Solution Accelerators - Security and Compliance team at Microsoft Corporation. One of her team's main objectives is to help remove security-related roadblocks to the adoption and deployment of Microsoft technologies. Chase Carpenter is a Product Unit Manager for Microsoft's Solution Accelerator Team. This team focuses on creating freely available tools, guidance, and automation that help customers accelerate their adoption of Microsoft's products. He spearheaded the creation of Microsoft's Security Guides which have evolved into the Microsoft Security Compliance Management Toolkit.
2:00 - 2:30 pm	**The OpenSCAP Project** – Steve Grubb, RedHat and Kevin Sitto, G2 The Openscap project is an an open source effort stemming from a collaboration between Red Hat and G2. We will discuss the challenges we faced when designing an open source, cross platform implementation of the major SCAP standards and the design decisions the community made to overcome them. We will also provide an architecture overview, a high level explanation of the APIs, and discussion of how to participate in the community. Steve Grubb leads the Security Technologies Team at Red Hat. His team works on Security Certifications and Guidance as well as maintains many of the security tools that you find on Linux systems. Kevin Sitto is a senior member of the technical staff of G2, Inc., a Columbia, Maryland-based firm specializing in Network Security Engineering and Cyberanalytic Modernization for government and commercial clients. In his role at G2 Mr. Sitto is focused on developing and implementing innovative standards-based approaches to improve Computer Network Defense (CND) capabilities for government and commercial clients.
2:30 - 3:00 pm	**Public Sector Adoption of SCAP Panel** – Paul Bartock, Moderator Much of the initial work developing SCAP was focused on meeting the needs of the US government to make sense of vulnerability data and to improve compliance with requirements such as FISMA. Over time, private industry recognized the benefits of security automation to help manage their corporate networks. This panel will take a look at how public sector companies are using SCAP to centralize vulnerability management, apply SCAP standards to correlate and prioritize data, and to automate vulnerability management workflow across their organizations. Panelists include John Pescatore, VP Internet Security, Gartner, Inc., and Ari Miller.
3:00 - 3:15 pm	*Break, Vendor Expo Hall*

Day 3, Wednesday, October 28	
3:15 - 3:45 pm	**Automating the Continuous Compliance Process in the Decentralized Enterprise** – Bill Niester, Qualys The evaluation of the IT security posture of enterprise assets has made great strides with the development of common standards such as those specified under the SCAP program. However, with the commonality that these standards brings, comes the even greater challenge of how to apply them effectively across large, distributed and decentralized environments.The challenge of continuously monitoring all assets in the enterprise is one that is best addressed through the use of automation. Providing the ability to reliably and effectively schedule data scans while simultaneous providing access to contextual, relevant and actionable results are the keys to effective and timely resolution of security vulnerabilities. The methods, benefits and challenges in the various architectures for achieving these results will be discussed during this presentation. Bill Niester has been providing security expertise to both government and industry for the past 15 years. He has held positions as Chief Information Security Technologist and Director of Security Consulting over the past 10 years and currently is the Director of Public Sector Markets for Qualys.
3:45 - 4:15 pm	**Automating Network Security Assessment** – Dr. Mike Lloyd, RedSeal Systems, Inc. and Doug Dexter, Cisco Errors in network security are one of the greatest threats to an organization. A large organization can have hundreds of thousands of interdependent firewall rules and router ACLs spread across hundreds of devices. A single subtle error or omission can expose the entire organization, yet easily be overlooked in an audit. This session discusses how network security can be automatically validated. It begins by covering how security policy can be documented at a higher level using security zones, white listing, black listing and incremental approvals. It then discusses how these policy-level checks can be automatically validated. Finally, it presents ideas for how network-wide security checks might be incorporated under the SCAP framework. Dr. Mike Lloyd, Chief Scientist, directs research into automated security assessment and network modeling for RedSeal Systems. Doug Dexter (Maj., USAR) is Cisco's internal Audit Team Lead, responsible for a global team of auditors who handle Cisco's acquisitions, vulnerability assessments, and site assessments.
4:15 - 4:45 pm	**Enhancing SCAP with Whitelist-based Image Management** – Wyatt Starns, SignaCert The Security Content Automation Protocol (SCAP) work is reaching an important juncture. The standards, framework, and capabilities embodied in SCAP to automate compliance can also be used as a foundational element to securely operate and manage networks. While the general focus, and to a large degree the external understanding of SCAP, has been around SCAP as a “Compliance” framework, with a key focus being security and vulnerability management, we are now realizing that SCAP is tremendous platform to create greater “real-time” operational visibility and control. The presentation will focus on ways we are extending SCAP vulnerably and configuration capabilities by adding state-of-art image management methods. It will include the use case, methods, and benefits of reference images derived from known-provenance software measurements (aka Whitelists) to gain unprecedented operational visibility and control with SCAP. Wyatt Starnes has more than 35 years in high technology, with eight startups. He is the Founder and CEO of SignaCert, Inc.
4:45 - 5:15 pm	**Vendor Interoperability Panel** – Andy Bove, Moderator This panel consists of a set of security tool vendors who would like to share their perspectives and experience with the SCAP standard. Lessons learned, unforeseen benefits, unforeseen social and technical challenges, and chance to hear what it is like to be a tool vendor that supports SCAP. Panelists include Tim Keanini, nCircle, Kent Landfield, Mcafee, Robert Hollis, Threatguard, Jonathan Frazier, Gideon Technologies, Nick Hansen, HP, and John Bordwine, Symantec.

5th Annual IT Security Automation Conference and Expo

October 26 - 29, 2009, Baltimore Convention Center

Focusing on Healthcare IT, Cyber Security, Regulatory Compliance, and other Emerging Secure IT Technologies

DoD Security Automation Strategy and Activities Track Abstracts

Day 2, Tuesday, October 27	
	This track will provide detailed insight into the DoD strategic security automation objectives and activities underway to achieve those objectives. The collection of presentations will describe a multitude of related standards and system development activities such as emerging security standards development, enterprise IT asset and vulnerability management infrastructure strategies and methodologies to include a discussion of the piloting activities underway to prove out the concepts and technical details of the underlying standards and architecture.
	Room 316/317
1:15 - 1:45 pm	**DoD Opening Discussion** This opening discussion will cover current issues and trends impacting the DoD security automation community and practices.
1:45 - 2:15 pm	**Consensus Audit Guidelines (CAG)** – Mason Brown, SANS *Wasting Money on Tools? What Really Works in Automating the Twenty Critical Security Controls* How much money have organizations spent on security products that end up on a shelf because they are too hard for “normal” people to make work or because they just don't solve the problems vendors promised they would solve? This briefing focuses on an innovative new initiative that promises to help ensure enterprises get effective value for the money they spend on security tools. The Twenty Critical Security Controls are rapidly becoming accepted as the best way to prioritize the activities necessary to actually improve security -- and to provide a baseline set of controls that can be continuously monitored through automated mechanisms. Mason Brown is one of a very small number of people in the information security field who have held a top management position in a Fortune 50 company. After earning his MBA from Harvard Business School, Mason joined Alcoa where he rose quickly to the President position for a $400 million division and then to a very senior executive role in a $5 billion division of Alcoa, with global responsibility. He brings this unique senior management perspective to the task of helping security professionals learn how to make a security program effective inside their organizations.

Day 2, Tuesday, October 27	
2:15 - 2:45 pm	**ARF, ARCAT, and Summary Reporting (T)** – LtCol Wolfkiel, NSA The DoD has been aggressively pursuing operational use of SCAP data standards for automated enterprise-wide network assessment and compliance reporting. In order to implement scalable reports that are interoperable across all vendors, two new languages, the Assessment Results Format (ARF) and Assessment Summary Results (ASR) have been created and are beginning implementation. ARF creates a separate XML record for each assessed device. An ARF device record includes installed applications and operating systems (using CPE), configurations of network interfaces, operational context, and SCAP compliance objects (XCCDF and OVAL XML documents). ASR is a summarization language for reporting counts or lists of assessed values of devices, including patches, vulnerabilities, OVAL definitions, XCCDF benchmarks, installed applications/operating systems, and other common assessment results. To demonstrate how ARF and ASR can be used in operational environments, the Assessment Results Collection and Analysis Tool (ARCAT) is being built as both a generic ARF consumer as well as a demonstration platform for producing ARF and ASR outputs based on fused multi-sensor inputs. This brief will provide an overview of ARF, ASR, and some lessons learned during the construction of ARCAT. Lt Col Wolfkiel has been the Computer Network Defense (CND) Research and Technology Program Management Office director since July 2006. His experience includes working at HQ US Strategic Command and HQ US Space Command as an Information Assurance (IA)/CND Staff Officer, working at the Air Force Communications Agency serving as the Chief IA Architect and as project lead for AF Office of Special Investigation’s enterprise Virtual Private Network (VPN), and the Air Force Enterprise VPN. He received a BS in Electrical Engineering from the University of Portland in 1989 and a Masters in Information Resource Management from AFIT in 1998.
2:45 - 3:15 pm	**ARF, ARCAT, and Summary Reporting (T) (continued)** – LtCol Wolfkiel, NSA
3:15 - 3:30 pm	*Break, Vendor Expo Hall*
3:30 - 4:00 pm	**CND Data Strategy (T)** – Shawn Oles and Sandra Harrell-Cook, NSA The CND Data Strategy piloting activities sponsored by the Office of Assistant Secretary of Defense for Networks and Information Integration (OASD NII) and the National Security Agency (NSA) Information Assurance Directorate, are focused on applying the Net-Centric data strategy to the CND mission to make CND data quickly visible, accessible, and understandable to people and systems across the DoD. The CND pilot works to achieve these goals by: 1) Building upon NIST SCAP data standards to create schemas that define how data is represented 2) Defining the interfaces through which data is exchanged, and 3) Validating the standards ability to support DoD missions and operations. The establishment and validation of CND data exchange standards is a necessary initial step in the transformation of a stove-piped, reactive and manual problem-solving environment to a flexible, powerful and net-centric environment.
4:00 - 4:30 pm	**CND Data Strategy (T) (continued)** – Shawn Oles and Sandra Harrell-Cook, NSA
4:30 - 5:00 pm	**Expanding the Use of SCAP: Malware Detection and MACE Tool Demo (T)** – Paul Green and George Saylor, G2 This session will cover how SCAP validated tools can be used to discover malware artifacts on government networks. We will demonstrate how to use the malware content editor (MACE) to develop the XCCDF/OVAL content to describe malware artifacts. This approach will dramatically reduce the time between when a new instance of malware and when it is detected on government networks. Paul Green is President and CEO of G2, Inc., a Columbia, Maryland-based firm specializing in Network Security Engineering and Cyberanalytic Modernization for the US government. Mr. Green graduated from the United States Merchant Marine Academy in 1996 with a BS in Engineering. Upon graduating Mr. Green focused on creating innovative solutions to identify, manage, and mitigate network vulnerabilities for national security clients. Mr. Green launched G2, Inc. in 2001 and quickly built a strong business base focusing on delivering trusted solutions for industry and various intelligence agencies.

Day 2, Tuesday, October 27	
5:00 - 5:30 pm	**Expanding the Use of SCAP: Malware Detection and MACE Tool Demo (continued) (T)** – Paul Green and George Saylor, G2

Day 3, Wednesday, October 28	
	Room 316/317
1:30 - 2:00 pm	**HBSS Open Framework Strategy** – Mark Orndorff
2:00 - 2:30 pm	**VMS/STIG SCAP Strategy (T)** – David Hoon, DISA *"DISA's Enterprise Strategy to Enhance Mission Assurance Capabilities using Data Standards"* This briefing will describe the current efforts that DISA is working on to automate configuration and vulnerability functionality and data exchange. The briefing will describe how standards-based capabilities will be used to improve situational awareness and mission assurance through the use of machine to machine communication and enterprise architectures. Details about specific tools and efforts will demonstrate how DISA is embracing data standards to improve the development of targeted and timely security guidance, to automate security assessments and reporting, and to improve knowledge about system risks and mitigations.
2:30 - 3:00 pm	**VMS/STIG SCAP Strategy (T) (continued)** – David Hoon, DISA
3:00 - 3:15 pm	*Break, Vendor Expo Hall*
3:15 - 3:45 pm	**Automating Attack Analysis Using Audit Data (T)** – Bruce Gabrielson, Booz Allen Hamilton This presentation will describe current efforts to collect, parse, normalize and extract platform generated audit date to detect attack signatures. Research related to identifying the optimum audit elements that need to be collected to support use cases, plus the process for creating the use cases themselves will also be presented. The ultimately deployed technology, including supporting languages, is expected to greatly enhance DoD's ability to use audit date for more effective situational awareness. Dr. Bruce C. Gabrielson is an Associate at Booz Allen Hamilton where he is the lead technical advisor for NSA's CND Research & Technology Program Management Office (I71). A certified telecommunications engineer, is listed as the inventor on three patents in the telecommunications industry, has published three technical books and well over one hundred technical papers. Involved with many leading edge technology research and development activities during his 40 year career, he also has many IA technology breakthrough solutions to his credit. He holds multiple advanced degrees in Business, Computer Science, and Electrical Engineering, and also a Teaching Credential in Math, Physics, and Physical Science. Most recently Dr. Gabrielson is involved with supporting the development of an Audit Management reference implementation system.
3:45 - 4:15 pm	**NETSPA (T)** – Steven Boyer

Day 3, Wednesday, October 28	
4:15 - 4:45 pm	**NSA Digital Policy** – Peter Sell, NSA This presentation discusses general issues related to digital policy management within an Enterprise. An overview of digital policy concepts, challenges, and a framework for addressing these challenges is discussed. Peter Sell works in the Enterprise IA Systems Engineering Services Office and has over twenty years of experience in Information Assurance. He is currently working on Enterprise Security Management, Digital Policy Management, and Access Control.
4:45 - 5:15 pm	**Remediation Specification (T)** – Matt Wojcik, Mitre In recent years, automated information security assessment for the enterprise has been revolutionized by the widespread adoption of SCAP. Enterprises can now precisely define policy for software inventory and configuration, vulnerability status, patch levels, etc. in a vendor-neutral way. There is a natural desire for similar capabilities for remediation. This presentation will provide an overview of a proposed remediation specification currently under development. Matthew Wojcik is a Lead Information Security Engineer at the MITRE Corporation. He has been involved with security standardization efforts at MITRE for the past ten years. Matt is currently project lead for CCE, and member of a team developing proposed specifications for remediation standardization. He was the original moderator of the OVAL Board, and is a past CVE analyst and past member of MITRE's IDS team. He is a frequent instructor of MITRE's Benchmark Development Course.

5th Annual IT Security Automation Conference and Expo

October 26 - 29, 2009, Baltimore Convention Center

Focusing on Healthcare IT, Cyber Security, Regulatory Compliance, and other Emerging Secure IT Technologies

Health IT and FIPS Track Abstracts

Day 2, Tuesday, October 27	
	The Health Information Technology (HIT) and FIPS track will explore the potential application of the SCAP suite of specifications to support security management, measurement, and regulatory compliance in healthcare and health IT computing environments. Health IT sessions will be conducted by NIST, the Centers for Medicare and Medicaid Services (CMS), and others. This track will also take a look at broad information technology topics, such as cryptography and identity management, that impact not only health IT but the larger IT landscape across all industries. Specific topics will include a survey of the identity management standards landscape, a discussion of strategies and considerations for transitioning towards stronger cryptography, a review of recent NIST cryptographic standards and guidelines, a status of the Cryptographic Hash Algorithm Competition, and an overview of the Cryptographic Module Validation Program.
	Room 318/319
1:15 - 1:45 pm	**NIST HIT Test Infrastructure Project** – Rob Snelick, NIST The American Recovery and Reinvestment Act (ARRA) of 2009 tasked NIST to establish a health IT standards testing infrastructure that supports effective industry consensus standards development processes and provides the U.S. healthcare IT industry and federal activities with robust conformance and interoperability testing capabilities. This session will discuss the objectives, scope, and requirements of this initiative, as well as the functional model, architecture, and scenario use cases. Robert Snelick is a computer scientist at the National Institute of Standards and Technology where he is the technical lead for the ARRA Healthcare Testing Infrastructure project and is a co-chair of the HL7 Implementation and Conformance technical committee. His technical focus is on developing tools for testing conformance and interoperability of healthcare data exchange standards.
1:45 - 2:15 pm	**Architecting Measurable Security in Health Information Technology Using SCAP** – Kenneth Lin and Daniel Steinburg, Booz Allen Hamilton This presentation uses a HIT use case to demonstrate how to architect measurable security using SCAP. For measurable security to be successful, an organization must understand risks it faces and select the right measurements. The presentation introduces a HIT Security and Privacy framework to analyze risks and derive the notional architecture that can drive the measurable security implementation. It then architects SCAP building blocks to demonstrate how measurable security can be implemented to manage risks on the given use case. Kenneth Lin is an Associate at Booz Allen Hamilton and Chief Security Architect for the National Cancer Institute's (NCI) ccaBIGR. He is a Health Information Exchange (HIE) Security and Privacy expert with extensive experience in designing large-scale federated security architecture to enable secure and private health information exchange using various standards. Daniel Steinburg is an Associate at Booz Allen Hamilton where he conducts legal and regulatory compliance analyses, including the privacy provisions of the Federal Information Security Management Act of 2002 and the Health Insurance Portability and Accountability Act (HIPAA) of 1996.

Day 2, Tuesday, October 27	
2:15 - 2:45 pm	**Centers for Medicare and Medicaid Services Case Study** – Ryan Brewer, CMS CISO This case study will discuss how the Centers for Medicare and Medicaid Services (CMS) is using SCAP-validated products in its operating environment, how the products are having an impact on CMS' operational security, compliance/audit management, and reporting across various regulatory frameworks (HIPAA, FISMA, CFO), future plans, lessons learned, automation functionality and future needs and capabilities. Ryan Brewer is currently the Chief Information Security Officer at the Centers for Medicare & Medicaid Services. Prior to CMS, Ryan worked at the Department of the Interior, where he served as the Trust Security Officer in the Department's Cyber Security Division.
2:45 - 3:15 pm	**Centers for Medicare and Medicaid Services Case Study (continued)** – Ryan Brewer, CMS CISO
3:15 - 3:30 pm	*Break, Vendor Expo Hall*
3:30 - 4:00 pm	**Cryptographic Transition Strategies** – Tim Polk, NIST Strong cryptography improves the security of systems and the information they process. However, as algorithms break or as computing techniques become more powerful, currently protected data may be left vulnerable. To address this challenge, organizations should proactively plan their transition strategy for migrating to stronger cryptographic algorithms. This session will discuss strategies and considerations for transitioning to stronger cryptographic protections, review recent NIST cryptographic publications, and provide an overview and current status of the Cryptographic Hash Algorithm Competition. Tim Polk has focused on computer security mechanisms at NIST since 1988. Tim currently is co-Security Area Director for the Internet Engineering Task Force (IETF). Past work includes the technical standards for Public Key Infrastructure (PKI) and the PKI underpinnings of FIPS 199 (the Personal Identity Verification Standard).
4:00 - 4:30 pm	**Cryptographic Validation Programs** – Randy Easter and Sharon Keller, NIST Federal agencies, industry, and the public rely on cryptography for the protection of information and communications used in electronic commerce, critical infrastructure, and other application areas. Although cryptography is used to provide security, weaknesses such as poor design of a cryptographic module or cryptographic algorithms that are implemented incorrectly can render the product insecure and place highly sensitive information at risk. Adequate testing and validation of the cryptographic module and its underlying cryptographic algorithms against established standards is essential to provide security assurance. This session will discuss the value of using validated cryptography, the objectives of the Cryptographic Module Validation Program (CMVP) and Cryptographic Algorithm Validation Program (CAVP), and their role and applicability in providing cryptography suitable for protecting sensitive information. Mr. Easter is the Director of the NIST Cryptographic Module Validation Program (CMVP). He joined NIST's Computer Security Division in 2000 and named the Director of the NIST CMVP in 2003. His duties include the validation of commercial cryptographic modules, editor and author of cryptographic and security guidance and standards including international standards, and is trained as an ISO 9000-2000 lead auditor. Ms. Sharon Keller has worked as a Computer Scientist for the U.S. Federal Government since October of 1983. She joined NIST in 1988 and has worked on the Cryptographic Algorithm Validation Program (CAVP) for the majority of her career. She was named the Director of the NIST CAVP in 2004 where she is responsible for the design and development of the validation tests for NIST-approved cryptographic algorithms.
4:30 - 5:00 pm	**Cryptographic Validation Programs (continued)** – Randy Easter and Sharon Keller, NIST

Day 2, Tuesday, October 27	
5:00 - 5:30 pm	**Secure and Scalable RESTful Health Data Exchange** – Gerald Beuchelt, MITRE Health data interoperability issues limit the expected benefits of Electronic Health Record (EHR) systems. Ideally, the medical history of a patient is recorded in a set of digital continuity of care documents which are securely available to the patient and their care providers on demand. To meet these requirements we have proposed hData, a simple XML-based framework for describing and exchanging health information using a RESTful architectural style. Electronic health data is aggregated through standard lightweight technologies such as Atom feeds, and kept on the EHR systems of providers, payers, and other actors. A discovery component allows patients to federate different EHR systems and manage access across the system through an OAuth based authorization approach. Gerald Beuchelt is a Lead Software Systems Engineer at the MITRE Corporation. He is focusing on advanced web services and identity management technology and their application in the context of complex government programs such as Health Care. In this role he is actively engaged with the identity and privacy management communities.

5th Annual IT Security Automation Conference and Expo

October 26 - 29, 2009, Baltimore Convention Center

Focusing on Healthcare IT, Cyber Security, Regulatory Compliance, and other Emerging Secure IT Technologies

Computer Network Monitoring, Audit, and Logging Track Abstracts

Day 2, Tuesday, October 27	
	This track provides an overview into recent research and advancements in standards related to networks, logging, and audit management. Presentations include potential use cases for these standards, emerging standards in the field, as well as some key benefits and challenges.
	Room 324/325
1:15 - 1:45 pm	**Insider Threat Panel** – Bruce Gabrielson, Moderator The panel will discuss the current state of insider threat detection and how standards might improve the field. Industry experts from government, industry and DoD will entertain questions and offer opinions on the subject. Panelists include Dr. Michael Glass, Chief of the Technical Counterintelligence Section for the National Counterintelligence Center and Greg Stevens, MITRE
1:45 - 2:15 pm	**Developing an SCAP Solution for Unified Communications** – Lawrence Dobranski, Nortel Networks, John Nagengast, AT&T, and Ben Halpert, Lockheed Martin Economic benefits have driven many organizations to migrate corporate communications to the Internet. While this typically saves organizations large amounts of money, potentially significant security, legal and compliance issues are all introduced due to the business mode, and this is especially significant for voice communications. From an enterprise voice perspective SCAP addresses three critical areas in providing a solutions level of assurance, namely, the management of security vulnerabilities, the management of corrective content (patches), and the management of security configuration. The ISAlliance designed a sophisticated project to develop an industry led, cost effective solution for these emerging issues based on SCAP technology. This executive session will provide a high level overview of the first phase of the ISAlliance VoIP SCAP project from the perspectives of a manufacturer, common carrier and enterprise user.

Day 2, Tuesday, October 27	
2:15 - 2:45 pm	**Using SCAP for Automated VoIP Configuration, Assurance and Security** – Paul Sand, Salare Security, LLC As Chair of the ISAlliance VoIP SCAP Applicability working group, Mr. Sand will provide a detailed report and presentation on the results and findings on behalf of this ISAlliance group. The number of VoIP endpoints rival the number of desktop computers that require management and thus is fertile ground for potential use of SCAP automation. Application of SCAP to a distributed, network wide application/service presents challenges never imagined as SCAP was designed to merely address desktops. Learn what aspects of SCAP can be directly ported to this distributed, network wide environment, what aspects require enhancement to maximize their utility and what new features are desirable to fully unleash the power of SCAP into such a complex environment. This presentation will present the VoIP Reference Architecture used in the study, an example VoIP Threat Risk Analysis and suggested VoIP Security Controls to support this effort. Then, use of the SCAP protocols and tools is examined in automating security control checking for the VoIP security controls. Finally, interesting new areas of study and further research will be considered.
2:45 - 3:15 pm	**Baseline Standards for Applying SCAP to Secure VoIP** – Mark Humphrey, Boeing, and Scott Armstrong, Gideon Technologies As Co-Chairs of the ISAlliance VoIP SCAP Baseline Standards working group, Mr. Humphrey and Mr. Armstrong will provide a detailed report and presentation on the results and findings on behalf of this ISAlliance group. The complexity of an enterprise VOIP implementation, and the required security controls, increases the number of baselines standards that must be considered when considering application of SCAP for assessment of VOIP Security. The use case of securing the Federal Desktop Core Configuration (FDCC) required consensus from many organizations and a few baseline standards for two host platforms from a single vendor. The use case for securing an enterprise VOIP implementation spans network and host platforms from multiple vendors, and applications from multiple vendors. This increases the level of effort significantly when attempting to perform a security assessment, and also increases the significant savings that leveraging SCAP for automation could provide. This presentation will include a VOIP Reference Architecture and Phone Security Overview used in the study, and a review of the common VOIP security control items used for baseline standards research, as well as the set of reference baseline standards collected as a result of this research.
3:15 - 3:30 pm	*Break, Vendor Expo Hall*
3:30 - 4:00 pm	**Common Event Expression (CEE) (T)** – Bill Heinbockel, Mitre This presentation discusses the Common Event Expression (CEE) effort. CEE is a framework to enable collaborative efforts in the creation of an open, practical, and industry-accepted event interoperability standard for electronic systems. The CEE effort is a coordinated industry initiative, developed by a community of vendors, researchers, and end users. This talk will frame the existing problem with current logging solutions and the challenges it brings to awareness of events occurring on a network. Each of the CEE components will be discussed along with examples of how they can be leveraged to solve the problems described. We will also discuss the CEE relationship to the NIST Event Management Automation Protocol (EMAP) effort.
4:00 - 4:30 pm	**Log Standard Challenges** – Anton Chuvakin The presentation will discuss how to bring order (in the form of standards!) to the chaotic world of audit and event logging. It will give a brief introduction to logs and logging and explain how and why logs grew so chaotic and disorganized. Next it will cover why log standards are sorely needed. It will offer a walkthrough that highlights the critical areas of log standardization. Past failed standards will be looked at and their lessons learned. Finally, current logging standard efforts will be presented briefly.
4:30 - 5:00 pm	**NSA Audit Management** – Chip Lutz, Booz Allen Hamilton An overview of recent activity and related efforts.
5:00 - 5:30 pm	**Final Thoughts** – Kevin Bingham, NSA A reflection and key points from the track.

5th Annual IT Security Automation Conference and Expo

October 26 - 29, 2009, Baltimore Convention Center

Focusing on Healthcare IT, Cyber Security, Regulatory Compliance, and other Emerging Secure IT Technologies

Cloud Computing Track Abstracts

Day 2, Tuesday, October 27	
	From infrastructure to integration and on into innovation in service design and delivery, we will shine a bright light on the reality and the promise of cloud computing. In particular, we will focus that light on the inclusion and automation of security features and assurances. Most importantly, "talk" will be matched with "walk". Presenters will use demonstrations and illustrations to show what is practical for today, and what we can look forward to for tomorrow. At the end of the cloud computing track, we will all know what a cloud "feels like", not just what cloud words "sound like". The cloud computing track includes a healthy cross section of enterprises making important contributions to cloud service capability and security. Whether you are intrigued by big companies with a long history of technology development or small companies with brand new ideas and offerings, they are both here. If you want to know how developers, integrators, and standards bodies are responding, they are all here too. And if you want to know the latest position and activities of government for cloud computing, you will find that here as well.
	Ballroom II
1:15 - 1:45 pm	**A Vision for a Private Cloud** – David Hunter, VMWare, Kunjal Trivedi, Cisco, and Nicklous Combs, EMC Federal Join Cisco, EMC and VMware for an overview of the integrated solution for the private cloud capabilities from each of the three companies. These 3 industry leaders will provide a detailed perspective of a fully virtualized datacenter to allow for a private cloud service. This includes virtualization of the IT infrastructure, the tie in with the servers and networking components to provide policy based services from end to end, and the storage and management requirements for the flexibility in virtual datacenter system deployments now and in the future. David Hunter is VMware's Chief Technology Officer for Public Sector where he functions as a senior technical liaison between VMware and the public sector community, evangelizing virtualization's value to improving the business of government and education. Kunjal Trivedi joined Cisco in 1999 as a consulting engineer initially and then worked in product management covering Cisco IOS Software infrastructure security. Currently, he is helping Cisco shape a vision and strategy for data center and cloud based managed services. Nicklous Combs has more than twenty-six years of experience managing, leading, and developing Information Technology solutions for the Military, Intelligence, Federal Government and commercial sectors. He is currently the Chief Technology Officer for EMC Federal.
1:45 - 2:15 pm	**A Vision for a Private Cloud (continued)** – David Hunter, VMWare, Kunjal Trivedi, Cisco, and Nicklous Combs, EMC Federal

Day 2, Tuesday, October 27	
2:15 - 2:45 pm	**App-Centric Scalability, Reliability, and Security in the Cloud** – Prakash Sinha, Citrix As web applications have evolved from simple publishing applications to the rich, highly interactive Web 2.0 applications of today, delivered on-premise or via cloud, ensuring their performance, security and availability has become both more important and more complex. Web 2.0 and Software-as-a-Service (SaaS) applications use internet technologies such as HTML, XML, JSON, and HTTP and may expose sensitive data over the Internet. This session discusses (and demonstrates) how virtualized network appliances, a complementary solution to hardware network appliances, are creating new deployment architectures that enables IT departments to implement application availability, security and acceleration services on-demand anywhere within private or hosted/cloud-based networks and data centers. Prakash Sinha is the Director of Product Management for Citrix.
2:45 - 3:15 pm	**Security Challenges in Cloud Computing** – Hasan S. Alkhatib, Microsoft Cloud Computing platform is a set of network accessible computing resources that are managed automatically as a computing utility service. Its goal is to deliver compute, storage, and connectivity services that scale-out on demand, and are resilient and highly available. The technology is disruptive in that it can potentially reduce TCO for computing services, relative to traditional datacenter-based computing, by an order of magnitude, through automation and improved utilization of the underlying physical resources. Cloud computing presents new security challenges across multiple dimensions. A public cloud computing service is characterized by multi-tenancy over shared physical resources. Furthermore, computations often require access to resources that reside beyond the cloud, including those inside enterprise private networks, while enterprises require protected private access to resources inside the cloud as well. Traditional datacenter security measures are insufficient to meet privacy and data protection requirements and compliance with regulation. This talk will identify security challenges in cloud computing and possible approaches to mitigate them. Hasan Alkhatib is a member of the Microsoft Windows Azure Enterprise Strategy team specializing in networking, network security, and regulatory compliance. He joined Microsoft in 2007 as General Manager of Enterprise Networking.
3:15 - 3:30 pm	*Break, Vendor Expo Hall*
3:30 - 4:00 pm	**An Accredited Fed Cloud IaaS** – Pete Nicoletti, Terremark This advanced technical presentation will discuss Terremark's Federal Cloud Architecture and all of the security components that we integrate and how we operate them as well as how we support client provided equipment, storage, DR, connectivity and related technologies. Our Fed Cloud IaaS was the first to be Certified and Accredited to the NIST 800-53A "Moderate" Level due to our architecture, processes, instrumentation, security layers that all contributed to our ability to be successfully audited to this extensive control set. We will review our detailed Network Diagram and then log into each security portal associated with our instrumentation tools. We will show how our IaaS and associated tools can assure "Continuous Compliance" to NIST 800-53A so that our clients can validate that their environment remains compliant every day after the yearly C&A effort. We will discuss and show live examples of operating, large scale Fed Cloud environments. Pete Nicoletti is the VP of Security Engineering at Terremark. Pete is currently managing the Consulting, Project Development, Program Management, Vender Relationships and related efforts of Terremark’s Secure Information Systems Managed Security Initiatives and professional Services for Federal and Commercial opportunities.

Day 2, Tuesday, October 27	
4:00 - 4:30 pm	**Cloud Standards: Opening the Cloud** – Victor L. Harrison, Object Management Group (OMG) Board of Directors The Object Management Group (OMG) is the worlds largest standards consortia. As was done with SOA, the OMG has initiated an effort to specify a standard profile containing the attributes and necessary characteristics of Cloud architectures and solutions. This briefing will update attendees on the plan being followed by the OMG (along with our standards partners, e.g., OASIS, Open Cloud Consortium, OGF, the Cloud Security Alliance, and many others) to create a unified and uniform specification by which potential customers of cloud computing can assess a particular implementation, permit both builds of cloud solutions and consumers of cloud solutions a uniform and consistent way of specifying capabilities, speed the enablement of cloud solutions, and assure that applications are designed to take advantage of Cloud Features. Victor L. Harrison leads CSC's public sector Distinguished Engineering Group, is a member of the Board of Directors of the Object Management Group, and is also a member of the Advisory Board of the SOA Consortium. In these capacities he provides leadership to CSC's engineering community, CSC's customers, and to the industry as a whole.
4:30 - 5:00 pm	**Separating Perceptional from Real Security Concerns** – George Reese, enStratus The driving issue behind the security concerns--both real and perceived--with cloud computing is the loss of control associated with cloud computing. Who is getting access to my data? What are they doing with it? In addition, a lack of sufficient transparency pervades the cloud computing space. Encryption and user management combined with solid key management can help mitigate many of the concerns in this area. George Reese, author of "Cloud Application Architectures" from O'Reilly and CTO of enStratus, will discuss and show how you can separate your key management infrastructure from your data management infrastructure to develop a public cloud environment that can be secured in spite of the lack of control and transparency you may have with many providers. George Reese is the CTO of enStratus.
5:00 - 5:30 pm	**Why Automation and Interoperability is Critical to Cloud Success** – Charles Crouchman, Opalis Join us and learn how to standardize IT best practices and implement process automation to build a successful, compliant, dynamic cloud environment. During this session we will explore how Opalis IT process provides interoperability between your existing infrastructure and management tools to mitigate risk, decrease costs, mask complexity and improve operational efficiency. The session provides answers to the following questions: • Self Service: How do I control provisioning of cloud resources? • Security: How do I apply existing management best practices to the cloud? • Availability: How does lifecycle management improve cloud performance? • Charge Back/Billing: How do I understand and control cloud costs? Charles Crouchman is the Chief Technology Officer for Opalis. A respected leader within the enterprise systems management community, Mr. Crouchman is responsible for driving the product strategy and development direction for Opalis.

Day 3, Wednesday, October 28	
	Ballroom II
1:30 - 2:00 pm	**Into the Cloud with SCAP** – Ron Knode, CSC What prevents an enterprise scale explosion in cloud processing that matches the individual and SMB growth patterns that have already been recorded? For CSC, the answer lies in restoring visibility into and through the cloud, and an implementation program to reclaim transparency even in cloud processing is underway. This effort includes a number of Orchestration Core efforts to make visible the evidence of trustworthy processing that each cloud can provide, and includes the CloudTrust Protocol (CTP) to request and reply with elements of transparency. The CloudTrust Protocol itself uses SCAP as a packaging and expression technique for many of the elements of transparency. This session includes a discussion of how this transparency is reintroduced and concludes with a brief demonstration scenario so the attendees can get a sense of what such transparency will look like and how it can make a difference in cloud usage. Ron Knode is a Director in the Global Security Solutions (GSS) business unit of CSC. In 2007 Ron was also named a Research Associate in CSC's internal "innovation think tank", known as the Leading Edge Forum (LEF). As the security architect for CSC's corporate cloud computing initiative (Trusted Cloud Services), Ron is examining and defining how the principles and practices of digital trust can be used to deliver their payoff potential through cloud processing models as well as traditional processing models.
2:00 - 2:30 pm	**Using SCAP to Mitigate Risks in the Cloud** – Ron Ritchey, Booz Allen Hamilton The potential cost savings and flexibility advantages of operating in cloud computing environments (CCEs) are compelling. However, cloud users need to understand the security risks, compliance complications, and potential legal issues inherent in CCEs. Federal agencies desiring to take advantage of cloud computing benefits will need to invest in proactive and strategic management of the new environment. Use of operating system images by CCE providers may introduce risks to CCE users and their organizations. This session will demonstrate how SCAP tools can be used to support Cloud Computing security governance of provider OS images. Ron Ritchey is a Principle at Booz Allen Hamilton and Chief Scientist of the Information Assurance Technology Analysis Center (IATAC).
2:30 - 3:00 pm	**Security as a Service** – Scott Chasin, McAfee Even though the term "Security as a Service" is brand new, products in this space have been evolving for almost a decade. In this talk, we'll show how security vendors are providing customers value by leveraging the cloud. We will look at the wide range of security offerings available today, and look at the value customers find in having such solutions in the cloud. For instance, we will look at cloud-based vulnerability assessment services, and show how they work with existing assessment standards such as OVAL, CVE and CVSS, while saving time and money through their deployment model. Another way vendors are leveraging the cloud is to better collect, analyze and distribute threat information. We will also look at cloud-based intelligence technologies and show the dramatic impact they are capable of having in our fight to protect the world from bad guys. Scott Chasin is the CTO at McAfee.
3:00 - 3:15 pm	*Break, Vendor Expo Hall*
3:15 - 3:45 pm	**New Advances in Virtualization Security Enable Secure Cloud Computing** – Aaron Bawcom, Reflex Systems While cloud computing has the potential to optimize infrastructure resources, improve the reliability of services, and reduce costs, many are still wary of embracing Cloud infrastructure due to the lack of security. Recent advances in virtualization security allow granular operational and network security controls via simple, dynamic policy rules. A new security model has been developed that enables IT organizations to leverage virtualization technologies to create and enforce "zones of trust" which can move dynamically into the Cloud while effectively preserving an organization's security posture. Bring an open mind and come see a demonstration of how this paradigm shift in security changes the game and enables Secure Cloud Computing. Aaron Bawcom is the VP of Engineering at Reflex Systems.

Day 3, Wednesday, October 28	
3:45 - 4:15 pm	**Cloud-enabled Protection of Data Integrity and Authenticity of Electronic Content** – Tom Klaff, Surety, LLC Data integrity and authenticity is a bet-the-business issue… The pressure is mounting to prevent and detect electronic record fraud. The trouble is that tampering with electronic records, files and other critical digital content has never been easier – all it takes is motive and a keystroke. With the massive volumes of electronic data now being created across your organization, and managed and stored by cloud computing platform providers, can you assume the risk of losing a legal or regulatory dispute because you cannot defend the integrity and authenticity of your electronic records, particularly those that contain your critical intellectual property content? This session will explore the importance of the preservation of electronic evidence that many cloud computing platform providers face when dealing with “chain of custody” issues surrounding customer content. This has deep implications for government (civilian and DoD), health and information agencies, as well as organizations in the private sector that host their trusted content with third-party providers. Attend this session and learn about the risks, the court cases, and the case studies surrounding electronic records and their vulnerability to manipulation. Learn how you can protect the integrity and legally defend the authenticity of your electronic content across the Cloud to cost-effectively mitigate this risk today and in the future. Tom Klaff is the CEO of Surety, LLC.
4:15 - 4:45 pm	**Endpoint Data Protection Services** – Gary Sumner, DataCastle Corporation Delivering PC Backup and other policy based endpoint data protection services utilizing a SaaS based model through the cloud. We will take you through the lessons learned and the key requirements for delivery of large scale, multi-tenant PC Backup and other policy based endpoint data protection services. We will show how you can still utilize the cloud as a delivery model with all its benefits, yet still keep tight centralized control with security and privacy maintained across your data even though it is now stored "outside" the traditional network boundary. Gary Sumner is the Founder and CTO of DataCastle Corporation. He has 20 years of experience in the design, development, and implementation of technology solutions across multiple industries.
4:45 - 5:15 pm	**The Cloud Architecture Tranformation** – Jim Blakley, Intel Corporation Whether you build your own cloud or use someone else’s, the underlying hardware and software architecture of the cloud matters. Performance matters, cost matters, security matters, reliability matters. And, a series of technology and architecture innovations are changing the way cloud builders design their data center infrastructure. This session will focus on some of the real world technology experiences and future challenges faced by the builders of public and private clouds as they design for virtualization, power optimization, solid state storage, converged network fabrics, large scale operations and the wide ranging applications that will land in their clouds. Jim Blakley is Director of Data Center Virtualization and Cloud at Intel. He leads technical and strategic engagements with enterprises and service providers in virtualization and cloud computing to enable technology adoption and understand future user needs. He works with Intel product teams and with the ecosystem to translate those needs to technology requirements and solutions.

5th Annual IT Security Automation Conference and Expo

October 26 - 29, 2009, Baltimore Convention Center

Focusing on Healthcare IT, Cyber Security, Regulatory Compliance, and other Emerging Secure IT Technologies

Compliance Frameworks/800-53/FISMA Track Abstracts

Day 3, Wednesday, October 28	
	There are many high-level sets of requirements for security, ranging from legislative and regulatory mandates and executive policy directives, to organizational policies and technical security configuration standards. Organizations must be able to demonstrate compliance with these requirements, including those specified by the Federal Information Security Management Act (FISMA) and the Federal Desktop Core Configuration (FDCC). Security automation, and more specifically the SCAP suite of specifications, SCAP-expressed checklists, and SCAP-validated tools, can be used to demonstrate conformance to many high-level policies and standards, including OMB and NIST security configurations and controls. Through use cases and technical discussions, the Compliance Frameworks track will explore the challenges, considerations, and lessons learned associated with the implementation of SCAP and FDCC. Sessions will also examine FDCC compliance and audit capabilities, discuss the current status of the FISMA implementation project activities, and explore the evolving NIAEC assessment methodology.
	Room 318/319
1:30 - 2:00 pm	**Understanding the Greatest FDCC Technical Challenges (T)** – Kurt Dillard Through the FDCC mailing list, agencies and vendors have identified all sorts of issues with the FDCC settings, using the virtual machines, and scanning computers. Kurt Dillard has been answering questions sent to the list for two years. In this session he will discuss the most common, as well as some less common but quite surprising, problems that have been uncovered. He will also present methods to resolve or work around each of these challenges. Kurt Dilliard is an independent consultant focusing on a variety of information security challenges for industry and the Federal government. He recently left Microsoft after many years of helping the company to develop and implement network security best practices. He has collaborated on many of the solutions published by Microsoft.
2:00 - 2:30 pm	**Understanding the Greatest FDCC Technical Challenges (T) (continued)** – Kurt Dillard

Day 3, Wednesday, October 28	
2:30 - 3:00 pm	**FISMA Implementation Project Update** – Arnold Johnson, NIST FISMA requires federal agencies to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency. FISMA reaffirmed NIST's role of developing information security standards and guidelines for non-national security federal information systems. To address its responsibilities under FISMA, NIST initiated the FISMA implementation project. This session will review the phases of the FISMA implementation project, and provide a current status of the security activities being conducted in each phase. Arnold Johnson is a senior Information Technology (IT) Security Researcher at NIST, where his work includes the development of standards, guidelines, and programs supporting FISMA implementation. His areas of specialization include IT security testing and evaluation, and information assurance.
3:00 - 3:15 pm	*Break, Vendor Expo Hall*
3:15 - 3:45 pm	**FDCC Compliance and Audit** – Kent Landfield, McAfee
3:45 - 4:15 pm	**FDCC Compliance and Audit (continued)** – Kent Landfield, McAfee
4:15 - 4:45 pm	**SCAP – Lessons Learned and an Enterprise Use Case** – Tony Uceda-Velez, Gideon Technologies Enterprise security depends on good, reliable, and up to date information. SCAP is a great standard to build upon for automating and standardizing our best practices for information security. However, large enterprise deployments of any technology has challenges, obstacles, opportunities that must be dealt with programmatically in order to maximize a project's success. This session will present the best practices and lessons learned from the deployment of SCAP tools enterprise wide the DHHS. Topics will include technical, organizational, and other lessons learned. This session should be of great interest of any agency or organization considering unifying security projects across a decentralized organization.
4:45 - 5:15 pm	**National Information Assurance Engagement Center (NIAEC)** – Wende Peters, Johns Hopkins APL The core underpinning of a NIAEC assessment is the ability to measure the effects of applying IA solutions and correlating those with mission impact. This presentation will explore the evolving methodology for NIAEC assessment and will include a short version of the current NIAEC demonstration, focusing on IA Best Practices. Wende Peters is the Director of the National Information Assurance Engagement Center (NIAEC) at the Johns Hopkins University Applied Physics Laboratory. Ms. Peters has an extensive background in systems engineering, with an emphasis on the architecture and design of large-scale, software-intensive systems. As the NIAEC Director, she focuses on the analysis of system vulnerabilities and their correlation to warfighter mission objectives.

5th Annual IT Security Automation Conference and Expo

October 26 - 29, 2009, Baltimore Convention Center

Focusing on Healthcare IT, Cyber Security, Regulatory Compliance, and other Emerging Secure IT Technologies

SCAP Technical Track Abstracts

Day 3, Wednesday, October 28	
	The SCAP Technical Track focuses on the technical challenges faced by the SCAP community. In addition to covering these challenges, sessions in this track will also explore possible solutions to these challenges. The solutions discussed will leverage proven SCAP technologies (e.g. XML) to address new problems. Some sessions will highlight solutions that will broaden the security automation technological environment by introducing new technologies (e.g. semantic technology) proven in other domains. All the sessions in this track focus on the technical aspects of security automation (both current and future) and it is expected that audience members will have a fairly good grasp of the technologies currently employed by the Security Content Automation Protocol.
	Room 324/325
1:30 - 2:00 pm	**Content Validation (T)** – Andy Bove, Secure Acuity As the adoption of the specifications has grown, an ecosystem that relies on content has evolved. In order for this ecosystem to flourish we must find ways of ensuring that the content that is created contributes to the "business of transacting information assurance" in a heterogeneous manner. This session will focus on how content validation supports the shared understanding necessary for this to happen, its similarities to other domains, and finally the status of the SCAP Content Validation Program being stood up by NIST. As the CTO for Secure Elements, Andy Bove contributed to the development of SCAP as well as the first enterprise implementation of the standard. As the founder of Secure Acuity Networks, Andy continues his commitment to the standards as the basis for protecting our nation's cyberspace, advising both the public and private sectors on all matters SCAP related.
2:00 - 2:30 pm	**Semantic Technologies Primer (T)** – Tim Keanini, nCircle Semantic technologies has been a frequent topic of conversation within many of the different individual communities. Some of the benefits of this technology are very intriguing and might offer solutions to some challenging problems. This session will introduce this technology and start exploring how individual initiatives might leverage it to their benefit. This session is recommended as a prerequisite for all individuals interested in the "Semantic Engineering / Modeling Panel" or the "Relational Database to Triple Store Migration" session. Tim Keanini's 19 years of technical expertise in the information security and gaming industries provides him with a unique perspective of customer challenges. As nCircle's CTO, Tim drives innovation and product strategy for the company. He is an active participant at the board and working group levels of several IT standards, some of them from their inception, and is driving for a day when consumers can have seamless automation across all of their vendor's products.
2:30 - 3:00 pm	**Semantic Technologies Primer (T) (continued)** – Tim Keanini, nCircle
3:00 - 3:15 pm	*Break, Vendor Expo Hall*

Day 3, Wednesday, October 28	
3:15 - 3:45 pm	**Semantic Engineering and Modeling Panel (T)** – Dave Waltermire, Moderator This panel will discuss the theory of semantic engineering and modeling; the focus will be on use cases where semantic technologies are being applied. Panelists are members of the community whom are currently involved with applying semantic technologies to real world problems. Panelists will first present an outline of the problem they are facing followed by an overview of how they are using semantic technologies to solve the problem. A questions and answer period will follow presentations. It is recommended that individuals interested in this panel attend the “Semantic Technologies Primer” session for an introduction to semantic technologies. Panelists include Paul Cichonski, Booz Allen Hamilton, Tim Keanini, nCircle, Matt Wojcik, Mitre, and Scott Streit. Paul Cichonski is a security professional and software engineer working for Booz Allen Hamilton. Currently, Mr. Cichonski is the co-lead developer for the National Vulnerability Database (NVD) at the National Institute of Standards and Technology (NIST). Mr Cichonski is heavily involved in the development of the Security Content Automation Protocol (SCAP). Tim Keanini’s 19 years of technical expertise in the information security and gaming industries provides him with a unique perspective of customer challenges. As nCircle’s CTO, Tim drives innovation and product strategy for the company. He is an active participant at the board and working group levels of several IT standards, some of them from their inception, and is driving for a day when consumers can have seamless automation across all of their vendor’s products. Matthew Wojcik is a Lead Information Security Engineer at the MITRE Corporation. He has been involved with security standardization efforts at MITRE for the past ten years. Matt is currently project lead for CCE, and member of a team developing proposed specifications for remediation standardization. He was the original moderator of the OVAL Board, and is a past CVE analyst and past member of MITRE's IDS team. He is a frequent instructor of MITRE's Benchmark Development Course. Scott Streit is an internationally recognized computer scientist with more than 25 years of experience as a technical leader/project manager. Currently, Mr. Streit is leading efforts for civilian agencies and corporate clients in the areas of semantic web and cloud computing.
3:45 - 4:15 pm	**Semantic Engineering and Modeling Panel (T) (continued**) – Dave Waltermire, Moderator
4:15 - 4:45 pm	**Semantic Engineering and Modeling Panel (T) (continued)** – Dave Waltermire, Moderator

Day 3, Wednesday, October 28	
4:45 - 5:15 pm	**Relational Database to Triple Store Migration (T)** – Vaibhav Khadilkar and Jyothsna Rachapalli, University of Texas at Dallas In addition to the theory behind semantic technologies it is also important to understand the implementation details. This session will focus on an ongoing joint effort between the National Vulnerability Database and the University of Texas at Dallas with the goal of migrating a portion of a relational database backed application to a semantic application backed by a triple store. This presentation will focus on strategies used, problems encountered, and metrics obtained throughout this migration. It is recommended that individuals interested in this panel attend the "Semantic Technologies Primer" session for an introduction to semantic technologies. Vaibhav is a Ph.D. candidate in the Department of Computer Science at the University of Texas at Dallas where he works in the Semantic Web and Cloud Computing labs. He earned his Masters in Computer Science from Lamar University in 2006. His primary interests are Semantic Web, Cloud Computing and Cryptography. His current work includes creating extensions for the Jena platform that enable creation of very large RDF graphs using Semantic Web and Cloud Computing technologies. Jyothsna Rachapalli is a doctoral student at The University of Texas at Dallas. She received her Master's degree in Computer Science in May 2009 from UTD where she worked on geospatial data management in the semantic web lab. She currently works as a Teaching Assistant in the Department of Computer Science for courses such as Digital Forensics and Data Applications and Security. Her research interests include knowledge engineering, semantic algebras and reasoning algorithms.